



Aks–Grotendikova teorema I

– Uvod u teoriju modela –

Slavko Moconja

MATF

5.12.2025.

Definicija. Neka je F polje. *Polinomijalno preslikavanje* $\Phi : F^n \rightarrow F^n$ je preslikavanje oblika:

$$\Phi(a_1, \dots, a_n) = (p_1(a_1, \dots, a_n), \dots, p_n(a_1, \dots, a_n)),$$

gde $p_1(X_1, \dots, X_n), \dots, p_n(X_1, \dots, X_n) \in F[X_1, \dots, X_n]$.

Teorema (Aks 1968; Grotendik 1966).

Svako 1-1 polinomijalno preslikavanje $\Phi : \mathbb{C}^n \rightarrow \mathbb{C}^n$ je na.

Definicija. Za polje F , označimo sa $AG(F)$ iskaz:

Za svako $n \geq 1$, svako 1-1 polinomijalno preslikavanje $F^n \rightarrow F^n$ je na.

(Dakle, $AG(\mathbb{C})$ je Aks-Grotendikova teorema.)

Dokazaćemo:

Teorema A. Za svako konačno polje F važi $AG(F)$.

Teorema B. Za svaki prost broj p važi $AG(\overline{\mathbb{F}}_p)$.

Teorema C. Za svako algebarski zatvoreno polje F važi $AG(F)$.

Teorema D. Važi $AG(\mathbb{C})$.

Primetimo: Teorema A je trivijalna. Teorema D sledi iz teoreme C.

Definicija. Jezik $\mathcal{L}$ je skup simbola konstanti, funkcijskih simbola i relacijskih simbola.

Funkcijski i relacijski simboli imaju *arnost* ≥ 1 .

Primeri.

1. $\mathcal{L}_\emptyset = \emptyset;$ (jezik čistog skupa)
2. $\mathcal{L}_O = \{<\};$ (jezik uređenja)
3. $\mathcal{L}_{Gp} = \{*,^{-1}, e\};$ (jezik grupa)
4. $\mathcal{L}_{AGp} = \{+, -, 0\};$ (jezik Abelovih grupa)
5. $\mathcal{L}_{Rng} = \{+, \cdot, -, 0, 1\};$ (jezik prstena sa jedinicom)
6. $\mathcal{L}_{ORng} = \{+, \cdot, -, <, 0, 1\}.$ (jezik uređenih prstena)

Definicija. $\mathcal{L}$ -struktura je par $\mathcal{A} = (A, (s^{\mathcal{A}})_{s \in \mathcal{L}})$ gde:

- A je neprazan skup – *domen strukture*;
- $s^{\mathcal{A}} \in A$, ako je s simbol konstante;
- $s^{\mathcal{A}} : A^n \rightarrow A$, ako je s funkcijski simbol arnosti n ;
- $s^{\mathcal{A}} \subseteq A^n$, ako je s relacijski simbol arnosti n .

$s^{\mathcal{A}}$ je *interpretacija* simbola s .

Primeri:

1. $(\mathbb{N}, <), (\mathbb{Q}, <)$ – $\mathcal{L}_O$ -strukture;
2. $\mathbb{S}_X = (\{X \xrightarrow{\text{bij.}} X\}, e^{\mathbb{S}_X} = \text{id}_X, \cdot^{\mathbb{S}_X} = \circ, {}^{-1\mathbb{S}_X} = {}^{-1})$ – $\mathcal{L}_{Gp}$ -struktura;
3. $(\mathbb{Z}, +, \cdot, -, 0, 1), (\mathbb{Z}_n, +, \cdot, -, 0, 1), (\mathbb{Q}, +, \cdot, -, 0, 1), (\mathbb{R}, +, \cdot, -, 0, 1), (\mathbb{C}, +, \cdot, -, 0, 1)$ – $\mathcal{L}_{Rng}$ -strukture;
4. $(\mathbb{R}, +, \cdot, -, <, 0, 1)$ – $\mathcal{L}_{ORng}$ -struktura.

Definicija. Neka su $\mathcal{A}$ i $\mathcal{B}$ $\mathcal{L}$ -strukture. Preslikavanje $h : A \rightarrow B$ je *homomorfizam* ako:

- $h(c^{\mathcal{A}}) = c^{\mathcal{B}}$, za simbole konstanti $c \in \mathcal{L}$;
- $h(f^{\mathcal{A}}(a_1, \dots, a_n)) = f^{\mathcal{B}}(h(a_1), \dots, h(a_n))$, za funkcijske simbole $f \in \mathcal{L}$;
- $R^{\mathcal{A}}(a_1, \dots, a_n) \implies R^{\mathcal{B}}(h(a_1), \dots, h(a_n))$, za relacijske simbole $R \in \mathcal{L}$.

h je *utapanje* ako dodatno h je 1-1 i u poslednjoj tački važi $\iff$.

Na utapanje je *izomorfizam*.

Definicija. $\mathcal{A}$ je podstruktura od $\mathcal{B}$, $\mathcal{A} \leq \mathcal{B}$, ako je $A \subseteq B$ i inkluziono preslikavanje je utapanje:

- $c^{\mathcal{A}} = c^{\mathcal{B}}$;
- $f^{\mathcal{A}}(a_1, \dots, a_n) = f^{\mathcal{B}}(a_1, \dots, a_n)$, za sve $a_1, \dots, a_n \in A$;
- $R^{\mathcal{A}}(a_1, \dots, a_n) \iff R^{\mathcal{B}}(a_1, \dots, a_n)$, za sve $a_1, \dots, a_n \in A$.

Primeri.

1. $(\mathbb{N}, <) \leq (\mathbb{Z}, <) \leq (\mathbb{Q}, <);$
2. $(\mathbb{Z}, +, \cdot, -, 0, 1) \leq (\mathbb{Q}, +, \cdot, -, 0, 1) \leq (\mathbb{R}, +, \cdot, -, 0, 1) \leq (\mathbb{C}, +, \cdot, -, 0, 1).$

Komentar. Neka je $\mathcal{B}$ struktura i $A \subseteq B$ neprazan. A je domen podstrukture ako i samo ako A sadrži sve $c^{\mathcal{B}}$ i zatvoren je za sve $f^{\mathcal{B}}$. Specijalno, ako je $\mathcal{L}$ relacijski jezik, svaki neprazan podskup $A \subseteq B$ je domen podstrukture.

Komentar. Ako su $\mathcal{A}_0 \leq \mathcal{A}_1 \leq \mathcal{A}_2 \leq \dots$ strukture, tada je $A := \bigcup_{n=0}^{\infty} A_n$ domen jedinstveno određene strukture $\mathcal{A}$ takve da $\mathcal{A}_n \leq \mathcal{A}$ za sve n .

Definicija. $\mathcal{L}$ -term je reč izgrađena od simbola konstanti, funkcijskih simbola, promenljivih $(x, y, z, \dots)$ i pomoćnih simbola po sledećim pravilima:

- promenljive i simboli konstanti su termi;
- ako je f funkcijski simbol arnosti n i $t_1, \dots, t_n$ termi, onda je i $f(t_1, \dots, t_n)$ term.

Notacija. Sa $t = t(x_1, \dots, x_m)$ naglašavamo da su promenljive u termu t (neke od) $x_1, \dots, x_m$. Kraće pišemo $t = t(\bar{x})$.

Definicija. Vrednost terma $t = t(\bar{x})$ u strukturi $\mathcal{A}$ pri valuaciji promenljivih $[x_1 \mapsto a_1, \dots, x_m \mapsto a_m]$, $t^{\mathcal{A}}(\bar{a})$, definišemo sa:

- $t^{\mathcal{A}}(\bar{a}) = c^{\mathcal{A}}$ ako $t = c$;
- $t^{\mathcal{A}}(\bar{a}) = a_i$ ako $t = x_i$;
- $t^{\mathcal{A}}(\bar{a}) = f^{\mathcal{A}}(t_1^{\mathcal{A}}(\bar{a}), \dots, t_n^{\mathcal{A}}(\bar{a}))$ ako $t = f(t_1, \dots, t_n)$.

Komentar. Ako $\mathcal{A} \leq \mathcal{B}$ i $\bar{a} \in A^m$, $t^{\mathcal{A}}(\bar{a}) = t^{\mathcal{B}}(\bar{a})$.

Definicija. *Atomske $\mathcal{L}$ -formule* su:

- $\perp$ i $\top$;
- $t_1 = t_2$, gde su t_1 i t_2 termi;
- $R(t_1, \dots, t_n)$, gde su $t_1, \dots, t_n$ termi.

Definicija. *$\mathcal{L}$ -formule* se grade na sledeći način:

- atomske formule su formule;
- ako su φ i ψ formule, onda su i $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$ i $(\varphi \leftrightarrow \psi)$ formule;
- ako je φ formula i x promenljiva, onda su i $\exists x\varphi$ i $\forall x\varphi$ formule.

Definicija. Pojavljivanje promenljive u formuli φ je *slobodno* ako nije pod dejstvom kvantifikatora; inače je *vezano*.

Notacija. Sa $\varphi = \varphi(x_1, \dots, x_m)$ naglašavamo da su promenljive koje se pojavljuju slobodno u formuli φ (neke od) $x_1, \dots, x_m$. Kraće pišemo $\varphi = \varphi(\bar{x})$.

Definicija. Definišemo relaciju $\mathcal{A} \models \varphi(\bar{a})$, formula $\varphi = \varphi(\bar{x})$ je tačna u strukturi $\mathcal{A}$ pri valuaciji promenljivih $[x_1 \mapsto a_1, \dots, x_m \mapsto a_m]$, sa:

- ako $\varphi = \perp$, $\mathcal{A} \not\models \varphi(\bar{a})$; ako $\varphi = \top$, $\mathcal{A} \models \varphi(\bar{a})$;
- ako $\varphi = (t_1 = t_2)$, $\mathcal{A} \models \varphi(\bar{a}) \iff t_1^{\mathcal{A}}(\bar{a}) = t_2^{\mathcal{A}}(\bar{a})$;
- ako $\varphi = R(t_1, \dots, t_n)$, $\mathcal{A} \models \varphi(\bar{a}) \iff R^{\mathcal{A}}(t_1^{\mathcal{A}}(\bar{a}), \dots, t_n^{\mathcal{A}}(\bar{a}))$;
- ako $\varphi = \neg\psi$, $\mathcal{A} \models \varphi(\bar{a}) \iff \mathcal{A} \not\models \psi(\bar{a})$;
- ako $\varphi = \psi \wedge \theta$, $\mathcal{A} \models \varphi(\bar{a}) \iff \mathcal{A} \models \psi(\bar{a})$ i $\mathcal{A} \models \theta(\bar{a})$;
- ...
- ako $\varphi(\bar{x}) = \exists y \psi(\bar{x}, y)$, $\mathcal{A} \models \varphi(\bar{a}) \iff \mathcal{A} \models \psi(\bar{a}, b)$ za neko $b \in A$;
- ako $\varphi(\bar{x}) = \forall y \psi(\bar{x}, y)$, $\mathcal{A} \models \varphi(\bar{a}) \iff \mathcal{A} \models \psi(\bar{a}, b)$ za sve $b \in A$.

Definicija. $\mathcal{L}$ -rečenica je formula bez slobodnih pojavljivanja promenljivih.

Definicija. Struktura $\mathcal{A}$ je *model* za rečenicu φ ako $\mathcal{A} \models \varphi$.

$\mathcal{A}$ je model za formulu $\varphi(\bar{x})$ ako je model za rečenicu $\forall \bar{x} \varphi(\bar{x})$.

Definicija. $\mathcal{L}$ -teorija je skup $\mathcal{L}$ -rečenica.

Definicija. Struktura $\mathcal{A}$ je *model* za teoriju T , $\mathcal{A} \models T$, ako je $\mathcal{A}$ model za svaku rečenicu iz T .

Definicija. Teorija T je *zadovoljiva* ako ima model.

Definicija. $\mathcal{L}$ -formula φ i ψ su *logički ekvivalentne*, $\varphi \equiv \psi$, ako za svaku $\mathcal{L}$ -strukturu $\mathcal{A}$ važi:

$$\mathcal{A} \models \varphi \leftrightarrow \psi.$$

Teorema. Svaka $\mathcal{L}$ -formula φ logički je ekvivalentna formuli oblika:

- $Q_1 x_1 Q_2 x_2 \dots Q_n x_n \psi,$

gde su $Q_1, Q_2, \dots, Q_n$ kvantifikatori i ψ je *beskvantorna formula*.

Definicija. Za $\mathcal{L}$ -formulu oblika:

- $Q_1 \bar{x}_1 Q_2 \bar{x}_2 \dots Q_n \bar{x}_n \psi,$

gde $Q_1 \neq Q_2 \neq Q_3 \neq \dots$ i ψ je beskvantorna kažemo da je:

- Σ_n ako je $Q_1 = \exists$;
- Π_n ako je $Q_1 = \forall$.

$\Sigma_0 = \Pi_0$ = beskvantorne formule.

1. $\mathcal{A} \leq \mathcal{B}$ ako i samo ako $A \subseteq B$ i za sve beskvantorne formule $\varphi(\bar{x})$ i sve $\bar{a} \in A$ važi:

$$\mathcal{A} \models \varphi(\bar{a}) \iff \mathcal{B} \models \varphi(\bar{a}).$$

2. Ako $\mathcal{A} \leq \mathcal{B}$, $\varphi(\bar{x})$ je Σ_1 i $\bar{a} \in A$, onda:

$$\mathcal{A} \models \varphi(\bar{a}) \implies \mathcal{B} \models \varphi(\bar{a}).$$

3. Ako $\mathcal{A} \leq \mathcal{B}$, $\varphi(\bar{x})$ je Π_1 i $\bar{a} \in A$, onda:

$$\mathcal{B} \models \varphi(\bar{a}) \implies \mathcal{A} \models \varphi(\bar{a}).$$

4. Ako $\mathcal{A}_0 \leq \mathcal{A}_1 \leq \mathcal{A}_2 \leq \dots \leq \mathcal{A} := \bigcup_{n=0}^{\infty} \mathcal{A}_n$ i φ je Π_2 -rečenica, onda:

$$\mathcal{A}_n \models \varphi \text{ za (skoro) sve } n \implies \mathcal{A} \models \varphi.$$